IT Security Handbook

Media Protection

ITS-HBK- 2810.11-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

May 6, 2011
Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

1 Introduction and Background

1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).

1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.

1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy*, *NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.

1.4 - *NPR 2810.1, NASA Information Security Policy*, designates this handbook as a guide of NASA's Media Protection (MP) information security controls.

1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.

1.6 - The Media Protection control family relates to the secure use of information storage media. Storage media can take one of two forms – digital or non-digital. Non-digital media typically consists of paper, film, microfilm, microfiche, etc. Digital media is comprised of mobile computing devices, laptops, PDAs, "smart phones," and removable storage devices such as USB drives, flash drives, writeable CDs and DVDs, memory cards, external hard drives, storage cards, diskettes, magnetic tapes, external/removable hard drives, or any electronic device that can be used to copy, save, store and/or move data from one system to another.

1.7 - The objective of the control family is to prevent or mitigate data loss and/or unauthorized access to NASA information and information systems, due to a failure to secure media, or a failure to sanitize media prior to reuse or disposal.

1.8 - **Applicable Documents**

- *NPD 2810.1, NASA Information Security Policy*
- *NPR 1441.1, NASA Records Retention Schedules*
- *NPR 1600.1, NASA Security Program Procedural Requirements*
- *NPR 2810.1, Security of Information Technology*
- *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
- *ITS-HBK-0035, Digital Media Sanitization*
- *Department of Defense (DoD) 5220.22-M, DoD Media Sanitization Guidelines*
- *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
- *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
- *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
- *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
- *NIST SP800-88, Guidelines for Media Sanitization*

2 Media Access (MP-2)

2.1 - **Roles and Responsibilities**

2.1.1 *The Information System Owner (ISO) shall*:

2.1.1.1 - Ensure access to digital and non-digital media containing non-public NASA information is restricted to only authorized individuals.

2.1.1.2 - Ensure that all NASA information made available on media to the public at large is in accordance with the requirements of existing laws, applicable policies, and the requirements of the Public Affairs Officer (PAO).

2.1.1.3 - Analyze all documents planned for publication against the table in Appendix A and B to ensure that no inappropriate content is disseminated.

3 Media Marking (MP-3)

3.1 **Roles and Responsibilities**

3.1.1 *The ISO shall*:

3.1.1.1 Ensure media for information system operations, digital and non-digital, are marked appropriately in a manner consistent with organizationally defined values.

3.1.1.1.1 Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, compact disks, digital video disks, and portable computing devices) and non-digital media (e.g., paper, microfilm).

3.1.1.1.2 Markings shall include applicable indications of intended distribution and/or handling requirements (e.g., Sensitive But Unclassified (SBU) and Controlled Unclassified Information (CUI)).

4 Media Storage (MP-4)

4.1 **Roles and Responsibilities**

4.1.1 *The ISO shall*:

4.1.1.1 - Ensure media used for NASA information system operation and restoration, (e.g. backups, procedure manuals, etc.) is physically protected and securely stored in a controlled area.

4.1.1.2 - Ensure media storage in controlled facilities is stored in an area accessible only to designated individuals and/or in a locked container.

4.1.1.3 - Ensure, if stored media uses data at rest encryption:

4.1.1.3.1 - The strength of the cryptographic mechanisms is commensurate with the classification and sensitivity of the information;

4.1.1.3.2 - Cryptographic key management is established and maintained that provides the required protection and ensures the availability of the information in the event of cryptographic key loss by users; and

4.1.1.3.1 - Destruction of stored media is in accordance with *NIST SP 800-88* and *ITS-HBK-0035*.

4.1.1.4 - Ensure backup copies of operating system and other critical information system software is stored in fire-rated containers that are not collocated with the operational software.

5 Media Transport (MP-5)

5.1 **Roles and Responsibilities**

5.1.1 *The ISO shall*:

5.1.1.1 - Ensure information system media that are transported outside the area of a NASA controlled facility are:

5.1.1.1.1 - Encrypted in accordance with NASA policy and procedures using validated encryption solutions for digital media;

5.1.1.1.2 - Stored in locked containers;

5.1.1.1.3 - Handled only by custodians/couriers approved by the ISO, mail, or an ISO approved commercial transport or delivery service with an accountable tracking system and manifest included in shipment; and

5.1.1.1.4 - Documented in a formal log identifying the media, custodian, the time it was provided to the custodian, destination.

5.1.1.2 - Designate the custodian/courier that is authorized to provide the media transport.

6 Media Sanitization (MP-6)

6.1 **Roles and Responsibilities**

6.1.1 *The ISO shall*:

6.1.1.1 Ensure adherence to media sanitization requirements in accordance with *NIST SP 800-88* and *ITS-HBK-0035*.

6.1.1.1.1 To meet the minimum sanitization requirements, media sanitization personnel may need to use the practices and processes identified in *DoD 5220.22-M*, and other industry and government best practices.

6.1.1.2 Ensure non-digital sensitive information (e.g., SBU, CUI) media is sanitized/disposed of in accordance with *NIST SP 800-88*, *ITS-HBK-0035*, and *NPR 1600.1*.

6.1.1.3 Ensure a record of media sanitization is maintained using the "Media Sanitization Record Form" included in the *ITS-HBK-0035*.

6.1.1.4 Ensure all portable/removable storage media are sanitized in a manner consistent with organizationally defined values.

6.1.1.5 Ensure media with federal records are not sanitized/disposed of unless in compliance with *NPR 1441.1*.

7 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
MP	01	Media Protection Policy and Procedures	*Main*	*[1]*	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
MP	02	Media Access	*Main*	*[1]*	Reference	Types of digital and non-digital media with restricted access.	Any media where distribution/access is restricted by public law or directives.	Any media where distribution/access is restricted by public law or directives.	Any media where distribution/access is restricted by public law or directives.
MP	02	Media Access	*Main*	*[2]*	Reference	List of authorized individuals with access to restricted types of media.	Individuals identified as authorized for that specific information	Individuals identified as authorized for that specific information	Individuals identified as authorized for that specific information
MP	02	Media Access	*Main*	*[3]*	Reference	Security measures used to protect restricted media.	Marked as CUI, SBU, or equivalent.	Marked as CUI, SBU, or equivalent.	Marked as CUI, SBU, or equivalent.
MP	03	Media Marking	*Main*	*[1]*	Reference	List of removable media types exempt from media marking.		None	None
MP	03	Media Marking	*Main*	*[2]*	Refer	Necessary conditions for exempted items.			

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
MP	04	Media Storage	*Main*	*[1]*	Reference	Types of digital and non-digital media with physical controls and secure storage considerations.		Media with information considered critical (e.g. mission operations, needed for system restoration, security audits, investigations).	Media with information considered critical (e.g. mission operations, needed for system restoration, security audits, investigations).
MP	04	Media Storage	*Main*	*[2]*	Reference	List of controlled areas where physically controlled and securely stored media must be kept.		NASA controlled areas/secure environment.	NASA controlled areas/secure environment.
MP	04	Media Storage	*Main*	*[3]*	Reference	Security measures used to protect media which required physical controls and secured storage.		Secured in a locked container.	Secured in a locked container.
MP	05	Media Transport	*Main*	*[1]*	Reference	List of types of digital and non-digital media requiring protection and control during transport out of controlled areas.		Information system operation(s) media (e.g. log files, backups, image files, etc).	Information system operation(s) media (e.g. log files, backups, image files, etc).

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
MP	05	Media Transport	*Main*	*[2]*	Reference	Security measures used to protect media during transport out of controlled areas.		1. Mark media-documents as sensitive (SBU, CUI, etc) 2. Encrypted in accordance with NASA policy and procedures with validated FIPS 140-2 (as amended) encryption 3. Use a Locked container for transport (e.g. Locked briefcase for non-digital media and/or portable media) 4. Use ISO-approved courier, registered mail, or ISO-approved commercial transport 5. Maintain a formal log documenting the transport activities	1. Mark media-documents as sensitive (SBU, CUI, etc) 2. Encrypted in accordance with NASA policy and procedures with validated FIPS 140-2 (as amended) encryption 3. Use a Locked container for transport (e.g. Locked briefcase for non-digital media and/or portable media) 4. Use ISO-approved courier, registered mail, or ISO-approved commercial transport 5. Maintain a formal log documenting the transport activities
MP	06	Media Sanitization	*E 2*	*[1]*	Frequency	Test and verification of sanitization equipment and processes.			1/Year

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
MP	06	Media Sanitization	*E 3*	*[1]*	Reference	List of circumstances requiring sanitization of portable, removable storage devices.			1. When the device is first received and before initial use. 2. When the device has been out of positive-chain-of-custody of authorized system personnel

Appendix A – Examples of Information Appropriate for Public Release

Information Types	Examples
Documents Intended for General Dissemination	• The NASA Strategic Plan. • Strategic Plans and related documents. • Personnel locator information not covered by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data section. • Organizational information not covered by the Privacy Act or FOIA Exemption 6. • Directions to a Center and related information that meets the legitimate needs of the public wishing to visit our Centers. • Information intended by the Agency to assist the public in better understanding the Agency's history, organization, missions, programs, and projects. • Personal, work-related biographies may be made available on the network as long as they do not compromise any sensitive information concerning PII or any aspect of the project with which the individual may be associated.
Official Agency Web sites which provide Agency policy documents	• Agency policy documents via the NASA Online Directives Information System (NODIS). (Note: Some NODIS policy documents are restricted for release to individuals accessing NODIS from non-NASA web sites.)
Information released by the Agency and Center Public Affairs Offices	• Press releases and similar information. • Public service messages such as anti-drug campaign information.
Official Agency Information Approved for Release	• Information that must be made available electronically to the public per the provisions of the Electronic Freedom of Information Act. • Official Agency budget information to the level of detail approved for release by the CFO. • Information developed by the Agency to assist industry in doing business with NASA, including electronic commerce information that does not contain proprietary data or content sensitive information as per this document (e.g., Requests for Proposals (RFP) may be published, but offer or responses to RFPs or source selection information may not be published). • Vendor quotes as part of an electronic reverse auction.
Published Information	• Science and engineering information and data that comply with NASA's policy for publication (see NPR 2200.2). • NASA Standards Program information, including official Agency engineering and information technology standards.

Appendix B – Examples of Information Not Appropriate for Public Release

Information Types	Examples
Information critical to protecting NASA assets and personnel	• Computer passwords or pass phrases. • Computer network configurations or designs. • Identification of operating systems (vendor, product, and version) used on specific servers. • Internet Protocol addresses. • Telephone numbers for dial-up computer connections. • IT System capabilities (e.g., staffing levels, hours of operation) or limitations. • IT System security plans, risk analyses, system vulnerabilities, procedures, and controls methods. • IT System compromise information, including evidence data. • IT System security/auditing logs. • Names/telephone numbers that uniquely identify system administrators. • Physical security information such as key codes and cipher lock combinations and significant badging information, including pictures of NASA badges. • Internal Center maps, including labeled aerial views. • Technically-detailed schematics or drawings of utilities, networks, airfields, aircraft, and buildings. • Facility information, including detailed drawings, schematics, physical locations, staffing levels, and hours of operation. • Specific information on the composition, preparation, and storage locations or optimal use of hazardous materials, explosives, or bio-toxins. • Detailed disaster recovery plans. • Details on emergency response procedures, evacuation routes, or officials responsible for these issues. • Personnel locator information as contained in Center or Agency telephone books (e.g., mail stops or building numbers). • Internal Center policies and procedures that have unresolved content publishing issues. • Personnel locators (i.e., building and room numbers or other information which could be used to determine personnel whereabouts at a given point in time, e.g., calendar information). • Information on internal NASA-only or Center-only activities or events (e.g., picnics, symposiums), especially which specifies exact locations. • Non-work-related personal information (including links to personal web pages or resumes). • Date and time identification of security-sensitive events. • Video streaming or still images of locations where physical vulnerabilities might be exposed. • Information designated as Controlled Unclassified Information (CUI) • NASA Mission Essential Infrastructures data
Information protected by law	• National security information (classified information). • Personal information prohibited from disclosure by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data. • Personally Identifiable information (PII) This information includes information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. • Export-controlled information. • Technical innovations prior to release approval by patent counsel. • Proprietary information of the Government or others such as: • Information disclosing inventions and technical innovations, including software, protected under 35 U.S.C. 205 and FOIA Exemption 3, unless release is approved by Center Patent Counsel. • Trade secret information protected or prohibited from disclosure under the Trade Secrets Act (18 U.S.C 1905) or FOIA Exemption 4. • Copyrighted materials unless approved for publication by the copyright owner. • Investigative information. • Commercially-licensed software restricted in accordance with the license or agreement under which it was obtained. • Information protected by treaty or agreement. • Invention disclosures. • Source evaluation information. • Confidential financial data relating to contractors. • Other information determined non-releasable under FOIA. • International Traffic in Arms Regulations (ITAR). • Procurement sensitive information, such as vendor quotes (except vendor quotes as part of an electronic auction), attribution information or results, or negotiating positions.
Information protected by Government or Agency	• NASA-developed software (unless authorized). • Information characterized as "Administratively Controlled Information" (per NASA policy) or previously designated "For Official Use Only."

Information Types	Examples
policy or regulation	• Pre-decisional information such as the Agency budget prior to formal release.
Embargoed scientific, technical, launch or other mission information	• Launch-related information whose compromise may adversely impact safety or security.